# Pairings on Generalized Huff Curves

Abdoul Aziz Ciss and Djiby Sow

Laboratoire d'Algèbre, Codage, Cryptologie, Algèbre et Applications
Université Cheikh Anta Diop de Dakar, Sénégal
BP: 5005, Dakar Fann
abdoul.ciss@ucad.edu.sn,sowdjibab@yahoo.fr

**Abstract.** This paper presents the Tate pairing computation on generalized Huff curves proposed by Wu and Feng in [22]. In fact, we extend the results of the Tate pairing computation on the standard Huff elliptic curves done previously by Joye, Tibouchi and Vergnaud in [14]. We show that the addition step of the Miller loop can be performed in $1\mathbf{M}+(k+15)\mathbf{m}+2\mathbf{c}$ and the doubling one in $1\mathbf{M}+1\mathbf{S}+(k+12)\mathbf{m}+5\mathbf{s}+2\mathbf{c}$ on the generalized Huff curve.

**Keywords:** Tate pairing, elliptic curves, Huff curves, Miller algorithm.

## 1 Introduction

Pairing computations on elliptic curves were introduced in 1948 by Weil [21], but their utilization in cryptography is actually quite recent. In 1993, Menezes, Okamoto and Vanstone in [17] used the Weil pairing to convert the discrete logarithm on some elliptic curves to a discrete logarithm in some extension of the base field.
More recenttly, Frey and Rück [11] extends the results of Menezes *et al.* on an even wider category of elliptic curves but with the Tate pairing instead of the Weil pairing.
Sakai, Ohgishi and Kasahara [19] and Joux [14] proposed independently in 2000 two cryptosystems using pairings on elliptic curves. In fact, Joux presented a Diffie-Hellman look alike protocol, except it allows three entities (instead of two) to create and exchange a secret key. Sakai, Ohgishi and Kasahara studied the use of pairings in identity-based cryptosystems. The idea of ID-based cryptography was introduced in 1984 by Shamir [20]. It consist in cryptosystem where the the public key of each entity is directly linked to its identity, which removes the need for its certification by a trusted certification authority.
Boneh and Franklin in [4] and Cocks [8] proposed separately in 2001 two identity based encryption schemes, the first one use the Weil pairing, the second one uses properties of quadratic residues. Since then, cryptographic pairings and their applications in cryptosystems have caught numerous researchers attention, and new ID-based protocols have been presented frequently [3,5,6,7,18].
Since cryptographic pairings were gaining more and more importance, many

researchers lead studies to families of curves where pairings are efficiently computable [2,9,10,12,16], as well as studies on efficient algorithms to compute pairings [1,12].
In [15], Joye, Tibouchi and Vergnaud present efficient formulæfor computing the Tate pairing on Huff curves. Our contribution in this paper is to extend their results on generalized Huff curves proposed by Wu and Feng in [22]. In fact, we show that the Tate pairing on generalized Huff curves is as efficient as in ordinary Huff curves and is a good choice to implement ID-based cryptography.
The rest of the paper is organized as follows : in the next section,we recall some basic definition and notation on generalized Huff curves and the Tate pairing. In section 3, we give the main result of the paper, i.e. formulæfor computing the Tate pairing on generalized Huff curves.

## 2 Preliminaries

### 2.1 Generalized Huff curves

In [22], Wu and Feng extend the Huff elliptic curves by introducing the new form

$$\tilde{\mathcal{H}}_{a,b} : x(ay^2 - 1) = y(bx^2 - 1),$$

where $ab(a - b) \neq 0$. This new model contains the ordinary Huff curves as particular case.
If $a = \mu^2$ and $b = \nu^2$ are squares in $\mathbb{F}$, pose $x' = \nu x$ and $y' = \mu y$. Therefore, $\mu x'(y'^2 - 1) = \nu y'(x'^2 - 1)$.
That means all curves of the form $ax(y^2 - 1) = by(x^2 - 1)$ are included in the family of curves $x(ay^2 - 1) = y(bx^2 - 1)$, where $a$ and $b$ are quadratic residues in $\mathbb{F}$. Note that $\tilde{\mathcal{H}}_{a,b}$ is smooth if $ab(a - b) \neq 0$.

**Theorem 1.** *Let $\mathbb{F}$ be a field of characteristic different from 2, let $a$ and $b$ be two elements of $\mathbb{F}$, with $a \neq b$. Then, the curve*

$$\tilde{\mathcal{H}}_{a,b} : X(aY^2 - Z^2) = Y(bX^2 - Z^2)$$

*is isomorphic over $\mathbb{F}$ to the elliptic curve given by the Weierstrass equation*

$$V^2W = U(U + aW)(U + bW)$$

*via the transformations $\varphi(X, Y, Z) = (U, V, W)$, where $U = bX - aY$, $V = (b - a)Z$ and $W = Y - X$. The inverse application is given by $\psi(U, V, W) = (X, Y, Z)$, with $X = U + aW$, $Y = U + bW$ et $Z = V$.*

In affine coordinates, the Huff curve $x(ay^2 - 1) = y(bx^2 - 1)$ defined over $\mathbb{F}$ is isomorphic to the elliptic curve$y^2 = x(x + a)(x + b)$ over $\mathbb{F}$.

**Expression of the group law over $x(ay^2 - 1) = y(bx^2 - 1)$ :**

Let $y = y_1 + \lambda(x - x_1) = \lambda x + \mu$ be the equation of the line through $P_1$, $P_2 \in \tilde{\mathcal{H}}_{a,b}(\mathbb{F})$, where $\lambda$ is the slope of the line through $P_1$ and $P_2$. By the equation of the curve, we obtain $x(a(\lambda x + \mu)^2 - 1) = (\lambda x + \mu)(bx^2 - 1)$. Let $S = P_1 + P_2 = (x_3, y_3)$. Then,

$$P_1 + P_2 = \left( \frac{(x_1 + x_2)(ay_1y_2 + 1)}{(bx_1x_2 + 1)(ay_1y_2 - 1)}, \frac{(y_1 + y_2)(bx_1x_2 + 1)}{(bx_1x_2 - 1)(ay_1y_2 + 1)} \right).$$

Consider now the two points $P_1$ and $P_2$ in projective coordinates, ie. $P_1 = (X_1, Y_1, Z_1)$ and $P_2 = (X_2, Y_2, Z_2)$, and $U = O = (0, 0, 1)$ as the neutral element of the group law. Let $S = P_1 + P_2 = (X_3, Y_3, Z_3)$. Then,

$$\begin{cases} X_3 = \big(X_1Z_2 + X_2Z_1\big)\big(aY_1Y_2 + Z_1Z_2\big)^2\big(Z_1Z_2 - bX_1X_2\big), \\ Y_3 = \big(Y_1Z_2 + Y_2Z_1\big)\big(bX_1X_2 + Z_1Z_2\big)^2\big(Z_1Z_2 - aY_1Y_2\big), \\ Z_3 = (b^2X_1^2X_2^2 - Z_1^2Z_2^2)(a^2Y_1^2Y_2^2 - Z_1^2Z_2^2). \end{cases}$$

Let $\mathbf{m}$, $\mathbf{s}$ and $\mathbf{c}$ be respectively the costs of the multiplication, squaring and multiplication by a constant. Let $m_1 = X_1X_2$, $m_2 = Y_1Y_2$, $m_3 = Z_1Z_2$, $c_1 = bm_1$ et $c_2 = am_2$.

1. $m_4 = (X_1 + Z_1)(X_2 + Z_2) - m_1 - m_3, \quad m_5 = (Y_1 + Z_1)(Y_2 + Z_2) - m_2 - m_3$
2. $m_6 = (m_3 - c_1)(m_3 + c_2), \quad m_7 = (m_3 + c_1)(m_3 - c_2)$.

Therefore, $X_3 = m_4m_6(m_3 + c_2)$, $Y_3 = m_5m_7(m_3 + c_1)$ et $Z_3 = m_6m_7$. Thus, the addition of two points of the curve can be evaluated in $12\mathbf{m} + 2\mathbf{c}$, where $2\mathbf{c}$ represent the cost of the multiplications by the two constants $a$ and $b$.

These addition formulæ are complete. In other word, they can be used to compute the point $2P = (x_3, y_3)$ for a given point $P = (x_1, y_1)$. Thus,

$$x_3 = \frac{2x_1(ay_1^2 + 1)}{(bx_1^2 + 1)(ay_1^2 - 1)} \quad \text{and} \quad y_3 = \frac{2y_1(bx_1^2 + 1)}{(bx_1^2 - 1)(ay_1^2 + 1)}.$$

In projective coordinates, the point 2 can be evaluated in $7\mathrm{m} + 5\mathrm{s} + 2\mathrm{c}$ when working with $U = O = (0, 0, 1)$ as neutral element

### 2.2 Backgrounds on the Tate pairing

**Definition 1.** *Let $G_1$ and $G_2$ be finite abelian groups written additively, and let $G_3$ be a multiplicatively written finite group. A cryptographic pairing is a map*

$$e : G_1 \times G_2 \longrightarrow G_3$$

*that satisfies the following properties:*

1. *it is non-degenerate, ie for all $0 \neq P \in G_1$, there is a $Q \in G_2$ with $e(P, Q) \neq 1$, and for all $0 \neq Q \in G_2$, there is a $P \in G_1$ with $e(P, Q) \neq 1$*

2. *it is bilinear, ie for all* $P_1, P_2 \in G_1$ *and for all* $Q_1, Q_2 \in G_2$ *we have*

$$e(P_1 + P_2, Q_1) = e(P_1, Q_1)e(P_2, Q_1)$$

$$e(P_1, Q_1 + Q_2) = e(P_1, Q_1)e(P_1, Q_2)$$

3. *it is efficiently computable*

An important property that is used in most applications and that follows immediately from the bilinearity is $e([a]P, [b]Q) = e(P, Q)^{ab} = e([b]P, [a]Q)$ for all $a, b \in \mathbb{Z}$ and for all $(P, Q) \in G_1 \times G_2$.

The Tate pairing can be defined on an ordinary abelian variety. It induces a pairing on the $r$-torsion subgroup of the abelian variety for a prime order $r$.
Let $E$ be an elliptic curve defined over a finite field $\mathbb{F}_q$ of characteristic $p$. Let $n = \#E$ and $r > 5$ be a prime different from $p$ and $r|n$.

**Definition 2.** *The smallest integer* $k$ *with* $r|(q^k - 1)$ *is called the embedding degree of* $E$ *with respect to* $r$

*Remark 1.* If $k$ is the smallest integer with $r|(q^k - 1)$, the order of $q$ modulo $r$ is $k$. Furthermore, the smallest field extension of $\mathbb{F}_q$ that contains the group $\mu_r$ of all $r$-th roots of unity is $\mathbb{F}_{q^k}$.

Let $E$ be an elliptic curve over $\mathbb{F}_q$ of characteristic $p > 3$ given by a short Weierstrass equation

$$E : y^2 = x^3 + ax + b \quad a, b \in \mathbb{F}_q.$$

Let $r \neq p$ be a prime such that $r|n = \#E(\mathbb{F}_q)$ and let $k > 1$ be the embedding degree of $E$ with respect to $r$.

**Lemma 1.** *Let* $D = \sum_{P \in E} n_P(P) \in Div(E)$. *Then* $D$ *is a principal divisor if and only if* $deg(D) = 0$ *and* $\sum_{P \in E} [n_P](P) = 0$, *where the latter sum describes the addition on* $E$.

**Definition 3.** *Let* $E$ *be an elliptic curve over a finite field* $\mathbb{F}_q$ *of characteristic* $p$ *and let* $r \neq p$ *be a prime dividing* $n = \#E(\mathbb{F})$. *Let* $k$ *be the embedding degree of* $E$ *with respect to* $r$. *The reduced Tate pairing is a map*

$$\begin{aligned} e_r : E(\mathbb{F}_q)[r] \times E(\mathbb{F}_{q^k})[r] &\longrightarrow \mu_r \subseteq \mathbb{F}_{q^k} \\ (P, Q) &\longmapsto f_{r,P}(D_Q)^{(q^k-1)/r} \end{aligned}$$

*where* $P \in E(\mathbb{F}_q)[r]$ *is* $\mathbb{F}_q$*-rational point of order dividing* $r$ *represented by a divisor* $D_p$, *and* $Q \in E(\mathbb{F}_{q^k})[r]$ *is* $\mathbb{F}_{q^k}$*-rational point represented by a divisor* $D_Q$ *such that its support is disjoint from the support of* $D_P$, *and* $f_{r,P} \in \overline{\mathbb{F}}_{q^k}(E)$ *is a function on* $E$ *with* $\mathrm{div}(f_{r,P}) = rD_P$.

When computing $f_{r,P}(Q)$ , ie when $rD_P$ is supposed to be the divisor of the function $f_{r,P}$, we can choose $D_P = (P) - (O)$. The divisor $D_Q \sim (Q) - (O)$ needs to have a support disjoint from $\{O, P\}$. To achieve that, one may choose a suitable point $S \in E(\mathbb{F}_{q^k})$ and represent $D_Q$ as $(Q + S) - S$.
We need to compute $f_{r,P}$ having divisor $\mathrm{div}(f_{r,P}) = r(P) - r(O)$. Lemma 1 shows that for $m \in \mathbb{Z}$, the divisor $m(P) - ([m]P) - (m-1)(O)$ is principal, such that there exists a function $f_{m,P} \in \overline{\mathbb{F}}_q(E)$ with $\mathrm{div}(f_{m,P}) = m(P) - ([m]P) - (m-1)(O)$. Since $P$ is a $r$-torsion point, we see that $\mathrm{div}(f_{r,P}) = r(P) - r(O)$, and $f_{r,P}$ is a function we are looking for.

**Definition 4.** *Given $m \in \mathbb{Z}$ and $P \in E(\mathbb{F}_{q^k})[r]$, a function $f_{m,P} \in \overline{\mathbb{F}}_{q^k}(E)$ with divisor $\mathrm{div}(f_{m,P}) = m(P) - ([m]P) - (m-1)(O)$ is called a Miller function*

**Lemma 2.** *Let $P_1, P_2 \in E$. Let $l_{P_1,P_2}$ be the homogeneous polynomial defining the line through $P_1$ and $P_2$, being the tangent to the curve if $P_1 = P_2$. The function $L_{P_1,P_2} = l_{P_1,P_2}(X, Y, Z)/Z$ has the divisor*

$$\mathrm{div}(L_{P_1,P_2}) = (P_1) + (P_2) + (-(P_1 + P_2)) - 3(O).$$

**Lemma 3.** *Let $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, $Q = (x_Q, y_Q) \in E$. For $P_1 \neq -P_2$ define*

$$\lambda = \begin{cases} (y_2 - y_1)/(x_2 - x_1) & \text{if } P_1 \neq P_2, \\ (3x_1^2 + a)/(2y_1) & \text{if } P_1 = P_2. \end{cases}$$

*Then, the dehomogenization $(l_{P_1,P_2})_*$ of $l_{P_1,P_2}$ evaluated at $Q$ is given by*

$$(l_{P_1,P_2})_*(Q) = \lambda(x_Q - x_1) + (y_1 - y_Q).$$

*If $P_1 = -P_2$, then $(l_{P_1,P_2})_*(Q) = x_Q - x_1$.*

**Lemma 4.** *Let $P_1, P_2 \in E$. The function $g_{P_1,P_2} := L_{P_1,P_2}/L_{P_1+P_2,-(P_1+P_2)}$ has the divisor*

$$\mathrm{div}(g_{P_1,P_2}) = (P_1) + (P_2) - (P_1 + P_2) - (O).$$

The function $g$ can be used to compute the Miller function recursively as shown in the next lemma.

**Lemma 5.** *The Miller function $f_{r,P}$ can be chosen such that $f_{1,P} = 1$ and such that for $m_1, m_2 \in \mathbb{Z}$, it holds*

$$f_{m_1+m_2,P} = f_{m_1,P} f_{m_2,P} g_{[m_1]P,[m_2]P},$$

$$f_{m_1 m_2,P} = f_{m_1,P}^{m_2} f_{m_2,[m_1]P} = f_{m_2,P}^{m_1} f_{m_1,[m_2]P}$$

*Remark 2.* Special cases from the previous lemma
Let $m \in \mathbb{Z}$, then

1. $f_{m+1,P} = f_{m,P} g_{[m]P,P}$,
2. $f_{2m,P} = f_{m,P}^2 g_{[m]P,[m]P}$,
3. $f_{-m,P} = (f_{m,P} g_{[m]P}, -[m]P)^{-1}$.

**Algorithm 1** Miller's Algorithm

1: $R \leftarrow P$, $f \leftarrow 1$
2: **for** $(i = l - 1; i \geq 0; i - -)$ **do**
3: $f \leftarrow f^2.g_{R,R}(Q)$
4: $R \leftarrow 2R$
5: **if** $(r_i = 1)$ **then**
6: $f \leftarrow f.g_{R,P}(Q)$
7: $R \leftarrow R + P$
8: **end if**
9: **end for**
10: **return** $f^{(q^k-1)/r}$

Note that $f_{0,P} = 1$ for all $P \in E$ and $g_{P_1,P_2} = 1$ if $P_1$ or $P_2$ equals the point at infinity $O$. These formulas show that any function $f_{m,P}$ can be computed recursively as a product line functions. The functions are defined over the field of definition of $P$.

**Lemma 6.** *Let $P \in E(\mathbb{F}_q)[r]$ and $Q \in E(\mathbb{F}_{q^k})[r]$, $\notin E(\mathbb{F}_q)$, then the reduced Tate pairing can be computed as $e_r(P,Q) = f_{r,P}(Q)^{(q^k-1)/r}$.*

The above algorithm, well known as the Miller's algorithm, can be used to compute $f_{r,P}(Q)$ for $P \in E(\mathbb{F}_q)[r]$ and $Q \in E(\mathbb{F}_{q^k})[r]$ and $r = (r_l, r_{l-1}, \ldots, r_0)_2$ up to irrelevant factors lying a proper subfield of $\mathbb{F}_{q^k}$. Since $k > 1$, these factors are mapped to 1 by the final exponentiation.

*Remark 3.* Note that the functions $g_{R,R}$ and $g_{R,P}$ in steps 3 and 6 are fractions and that the inversions in each step of the loop can be postponed until the end of the loop by keeping track of numerator and denominator separately.

## 3 Pairing computation on generalized Huff curves

The Tate pairing computation on the classic Huff curves was introduced by Joye *et al.* in [15]. The main contribution of this paper is the extension of the previous results on the generalized Huff curves.

Huff curves can be represented as plane cubics. Thus, we can apply directly the Miller Algorithm to compute pairings on these curves. It's quite usual to represent the point $Q \in E(\mathbb{F}_{q^k})\backslash E(\mathbb{F}_q)$ in affine coordinates since, in the Miller algorithm, the function is always evaluated at the same point. Let $Q = (y, z) = (1 : y : z)$. Suppose the embedding degree $k$ is even, then $Q$ can be written in the form $Q = (y_Q, z_Q\alpha)$, with $y_Q, z_Q \in \mathbb{F}_{q^{k/2}}$, $\mathbb{F}_{q^k} = \mathbb{F}_{q^{k/2}}(\alpha)$, where $\alpha$ is a non quadratic residue in $\mathbb{F}_{q^{k/2}}$.
Let $P, R \in E(\mathbb{F}_q)$ and $l_{R,P}$ be the rational function vanishing on the line through $P$ and $R$. We have

$$l_{R,P}(Q) = \frac{(zX_p - Z_p) - \lambda(yX_p - Y_P)}{X_P}$$

where $\lambda$ is the $(y,z)$-slope of the line through $P$ and $R$. Then, the divisor of $l_{R,P}$ is given by

$$\mathrm{div}(l_{R,P}) = R + P + T - (1:0:0) - (0:1:0) - (a:b:0)$$

where is $T$ is the third intersection of the line through $P$ and $R$ with the curve. If $U$ is the neutral element of the group law $(+)$, then the function $g_{R,P}$ can be expressed as

$$g_{R,P} = \frac{l_{R,P}}{l_{R+P,U}}$$

Let $U = O = (0:0:1)$ be the neutral element of the addition law. Then, for all $Q = (y_Q, z_Q\alpha)$, we have

$$l_{R+P,O} = y_Q - \frac{Y_{R+P}}{X_{R+P}} \in \mathbb{F}_{q^{k/2}}$$

This quantity is equal to 1 after the final exponentiation in the Miller algorithm since it belongs to a proper sub-field of $\mathbb{F}_{q^k}$. That means it can be canceled in computations. In the same context, divisions by $X_P$ can be omitted, and the denominator in the expression of $\lambda$ too, ie. if $\lambda = \dfrac{A}{B}$, then the function $g_{R,P}$ can be evaluated as

$$g_{R,P}(Q) = (z_Q\alpha.X_p - Z_p)B - (yX_p - Y_P)A$$

We are now ready to give explicit and precise formulæ for the addition and doubling steps of each round of the Miller loop.

**Addition step**. In the addition step, the $(y,z)$-slope of line through the points $P = (X_P : Y_P : Z_P)$ and $R = (X_R : Y_R : Z_R)$ is given by

$$\lambda = \frac{Z_R X_P - Z_P X_R}{Y_R X_P - Y_P X_R}.$$

Therefore, the function to be evaluated is of the form

$$g_{R,P}(Q) = (z_Q\alpha.X_P - Z_P)(Y_R X_P - Y_P X_R) - (y_Q.X_P - Y_P)(Z_R X_P - Z_P X_R).$$

Since the points $P$ and $Q$ remain constant during the execution of the Miller loop, the values depending on $P$ and $Q$, ie. $y'_Q = y_Q.X_P - Y_P$ and $z'_Q = z_Q\alpha.X_P$ can be precomputed. Thus, each addition step of the Miller algorithm requires the calculation of $R + P$ (an addition over $E(\mathbb{F}_q)$), the evaluation of $g_{R,P}(Q)$, and the calculation of $f.g_{R,P}(Q)$ (a multiplication over the field extension $\mathbb{F}_{q^k}$). $R + P$ can be evaluated in $12\mathrm{m} + 2\mathrm{c}$ using the steps $M_1, M_2, \ldots, M_7$.
Let $m_8 = (X_R + Y_R)(X_P - Y_P)$ and $m_9 = (X_P + Z_P)(Z_R - X_R)$. Then,

$$g_{R,P}(Q) = (z'_Q - Z_P)(m_8 - m_1 + m_2) - y'_Q(m_9 + m_1 - m_3),$$

where the first term require $(\frac{k}{2} + 1)\mathbf{m}$, and the second one $\frac{k}{2}\mathbf{m}$. With the final multiplication in $\mathbb{F}_{q^k}$, the cost of an addition step is $1\mathbf{M} + (k + 15)\mathbf{m} + 2\mathbf{c}$.

**Doubling step.** In the doubling step, the slope of the tangent line to the curve at the point $R = (X_R : Y_R : Z_R)$ is given by

$$\lambda = \frac{aZ_R^2 - 2bY_RZ_R - X_R^2}{bY_R^2 - 2aY_RZ_R - X_R^2} = \frac{A}{B}.$$

Therefore,

$$g_{R,R}(Q) = z_Q\alpha.X_RB - Z_RB - y_Q.X_RA + Y_RA.$$

In the Miller algorithm, we need to compute the point $2R$, which can be done in $7\mathbf{m} + 5\mathbf{s} + 2\mathbf{c}$. $A$ and $B$ can be evaluated in $1\mathbf{m}$, namely $Y_RZ_R$ since the other terms are already computed with the doubling operation. Therefore, the function $g_{R,R}$ can be computed in $4\mathbf{m}$ ($X_RB$, $Z_RB$, $X_RA$ and $Y_RA$), $\frac{k}{2}\mathbf{m}$ for $z_Q\alpha.X_RB$ and $\frac{k}{2}\mathbf{m}$ for $y_Q.X_RA$. Thus, the doubling step require a total cost of $1\mathbf{M} + 1\mathbf{S} + (k + 12)\mathbf{m} + 5\mathbf{s} + 2\mathbf{c}$, by taking in account the multiplication, the squaring which complete the duplication.

## Conclusion

We have successfully extended the Tate pairing computation on generalized Huff curves introduced by Wu and Feng. Our results are not far from the standard case since the the multiplication by constant are often negligible. That makes it as efficient as the standard Tate pairing computation on Huff curves proposed by Joye, Tibouchi and Vergnaud. The next step is to use use result to design efficient cryptographic protocols such as ID-base protocols.

## References

1. P.Barreto, H.Kim, B.Lynn and M.Scott. *Efficient algorithms for pairing-based crytosystems*, 2002, Available at `http://eprint.iacr.org/2002/008/`.
2. P.Barreto, B.Lynn and M.Scott. *Constructing elliptic curves with prescribed embedding degree*, 2002, Available at `http://eprint.iacr.org/2002/008/`.
3. A. Boldyreva. *Efficient threshold signature multisignature and blind signature schemes based on the Gap-Diffie-Hellman group signature scheme*. 2002, Available at `http://eprint.iacr.org/2002/118/`.
4. D. Boneh and M. Franklin. *Identity-based encryption from the Weil pairing*. In J. Kilian, editor, Advances in Cryptology - CRYPTO 2001, LNCS volume 2139, pages 213-229, Spriner Verlag, 2001.
5. D. Boneh, B. Lynn and H. Shacham. *Short signatures from the weil pairing*. In C. Boyd, editor, Advances in Cryptology - ASIACRYPT 2001, LNCS volume 2248, pages 514-532, Spriner Verlag, 2001.
6. C. Castellucia. *How to convert any ID-based signature from Gap-Diffie-Hellman groups*, 2002, Available at `http://eprint.iacr.org/2002/018/`.
7. J. Cha and J. Cheon. *An identity-based signature form Gap-Diffie-Hellman groups*, 2002, Available at `http://eprint.iacr.org/2002/018/`.

8. C. Cocks. *An identity based encryption scheme based on quadratic residues*. In B. Honary, editor, Cryptography and Coding, LNCS volume 2260, pages 360-363, Spriner Verlag, 2001. 8th IMA International Conference, UK, 2001. Proceedings.
9. R. Dupont and A. Enge and F. Morain. *Building curves with arbitrary small mov degree over finite prime fields* 2002, Available at `http://eprint.iacr.org/2002/094/`.
10. Edwards, H.M., *A normal form for elliptic curves*. Bulletin of the American Mathematical Society 44 (2007), 393-422. Avalaible at `http://www.ams.org/bull/2007-44-03/S0273-0979-07-01153-6/home.html`.
11. G. Frey and H.-G. Rück. *A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves*. Math. Comp., 62(206):865-874, April 1994.
12. S. Galbraith. *Supersingular curves in cryptography*. In C.Boyd, editor, Advances in Cryptology-ASIACRYPT 2001, LNCS volume 2248, pages 495-513, Spriner Verlag, 2002. 7th International Conference on the theory and applications of cryptography and information decurity, Gold Coast, Australia, December 9-13, 2001, Proceedings.
13. S. Galbraith, K. Harrison and D. Soldera. *Implementing the Tate pairing*. In Algorithmic Number Theory Symposium - ANTS V, LNCS volume 2369, pages 495-513, 2002.
14. A. Joux. *A one round protocol for tripartite Diffie-Hellman*. In W. Bosma, editor, ANTS-IV, volume 1838, of lecture notes in comput. sci. pages 358-394, Spriner Verlag, 2000. 4th International Symposium, ANTS-IV, Leiden, The Netherlands, July 2-7, 2000, Proceedings.
15. M. Joye, M. Tibouchi, and D. Vergnaud. *Huff's Model for Elliptic Curves*. In G. Hanrot, F. Morain, and E. Thomé Eds, Algorithmic Number Theory (ANTS-IX), vol. 6197 of LNCS, pp. 234-250, Springer, 2010.
16. A. Miyaji, M. Nakabayashi and S.Takano. *New explicit conditions for elliptic curve traces for FR-reduction*. IEICE Trans. Fundamentals, E84- A(5):1234-1243, 2001.
17. A. Menezes, T. Okamoto and S. A. Vanstone. *Reducing elliptic curves logarithms to logarithms in a finite field*. IEEE Trans. Inform. Theory, IT-39(5):1639-1646, september 1993.
18. S.Al-Riyami and K.Paterson. *Authenticated three patry key agrement protocols from pairings* 2002, Available at `http://eprint.iacr.org/2002/035/`.
19. R. Sakai, K. Ohgishi and M. Kasahara. *Cryptosystems based on pairings*. SCIS 2000, the 2000 symposium on cryptography and information security, Okinawa, japan, January 26-28
20. A. Shamir. *Identity-based cryptosystems and signatures schemes*. In Advances in Cryptology-CRYPTO'84, LNCS volume 196, pages 47-53, Spriner Verlag 1985.
21. A. Weil. *Courbes algébriques et variétés abéliennes*. Hermann, 1948.
22. H. Wu, R. Feng. *Elliptic curves in Huff's model*, 2010, Available at `http://eprint.iacr.org/2010/390`.